The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Official Action dated November 19, 2004. In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due consideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

Claims 1-12 are under consideration in this application. Claims 1-12 are being amended, as set forth in the above marked-up presentation of the claim amendments, in order to more particularly define and distinctly claim applicant's invention.

Additional Amendment

The claims and the Abstract are being amended to correct formal errors and/or to better recite or describe the features of the present invention as claimed. All the amendments to the claims are supported by the specification. Applicant hereby submits that no new matter is being introduced into the application through the submission of this response.

Formality Rejection

The Abstract of the Disclosure was objected to for being in improper format, and claims 7 and 11 were objected to for minor informalities. Claims 1 – 12 were rejected under 35 USC §112, second paragraph, on the grounds that these claims were unclear. Specifically, the Examiner cited language in claims 1, 5 and 9 that required clarification.

As indicated, the specification and the claims have been amended as required by the Examiner. Accordingly, the withdrawal of the outstanding informality rejection is in order, and is therefore respectfully solicited.

Prior Art Rejections

Claim 1 was rejected under 35 U.S.C. §102(e) on the grounds of being anticipated by US Patent No. 6,219,791 to Blanchard et al. (hereinafter "Blanchard"). Under 35 U.S.C. §103(a),

claim 2 was rejected as being obvious over Blanchard in view of the article "Concurrent Error Detection In Block Ciphers" to Fernandez-Gomez et al.(hereinafter "Fernandez-Gomez"); claim 3 over Blanchard in view of US Application No. 2002/0178354 A1 to Ogg et al. (hereinafter "Ogg"); claim 4 over Blanchard in view of the article "On the Importance of Checking Cryptographic Protocols for Faults" to Boneth et al. (hereinafter "Boneth"); claims 5 and 6 over US Patent No. 5,991,401 to Daniels et al. (hereinafter "Daniels") in view of Fernandez-Gomez; claim 7 over Daniels in view of Fernandez-Gomez and Ogg; claim 8 over Daniels in view of Fernandez-Gomez and Boneth; claims 9 and 10 over Daniels in view of the publication "Applied Cryptography" to Schneier (hereinafter "Schneier"); claim 11 over Daniels in view of Schneier and Ogg; and claim 12 over Daniels in view of Schneier and Boneth. US Patent No. 5,608,798 to Likens et al. and US Patent No. 6,144,740 to Laih et al. were cited as being pertinent to the disclosure of the present invention. These rejections have been carefully considered, but are most respectfully traversed.

The tamper-resistant fault detection method (e.g., Fig. 5; pp. 14-15) for an IC card 101 (Fig. 1; p. 1, lines 5-6) including an information processing device 102 mounted thereon (e.g., a chip including a CPU therein; p. 1, lines 22-23; Abstract; "*A tamper-resistant apparatus represented by an IC card chip comprises a storage device having a program-storage portion which stores programs and a data-storage portion which stores data, and a central processing unit (CPU) which performs data processing by executing designated processes following the programs. The apparatus can be understood as an information processing device in which the programs, composed of processing instructions giving execution orders to the CPU, provide one or more data processing mean*" p. 6, lines 10-19), as now recited in claim 1, comprises the steps of: (1) performing a <u>symmetric-key encryption</u> process $Z = E (M, K)$ (e.g., DES, p. 11, lines 16-17) in which a secret key K is to be applied to an input plaintext M, and storing a processing result Z in a memory 204 in the IC card 101 (Fig. 2); (2) performing a corresponding decryption process $W = D (Z, K)$ for said process result Z stored on said memory 204 and storing the decryption result W on the memory 204; (3) outputting said processing result Z <u>from said information processing device</u> when said processing result W coincides with said plaintext M; and (4) <u>suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said plaintext M.</u>

The main purpose of the present invention is to prevent an attack on an encryption mechanism from successfully occurring so as to prevent an attacker's attempt to obtain the information of how the encryption mechanism processes data by acquiring both an incorrect result and a correct answer. For this purpose, the present invention is configured in such a manner that it prohibits the processing result from outputting out of the mechanism when the result proves incorrect (p.13, line 12 to p. 14, line 5, in particular, p.14, lines 4-5). If any error occurs caused by an erroneous operation in the DES processing result "intentionally" (p. 3, line 25; Abstract) generated by an attacker while an IC card is performing encryption processing (p. 4, lines 1-3), the error is surely detected by the observation of the decryption result such that the IC card get reset to suppress outputting of the processing result Z. As such, an attacker is not able to obtain any erroneous processing result which is necessary for an attack to execute an attack (p. 15, lines 11-17).

The invention, as now recited in claim 5, is directed to a tamper-resistant fault detection method (e.g., Fig. 6; pp. 15-16) for an IC card including an information processing device mounted thereon, that comprises the steps of: (1) performing a <u>symmetric-key decryption</u> process $Z = D (C, K)$ wherein a secret key K is to be applied to an input ciphertext C, and storing the processing result Z on a memory in the IC card; (2) performing a corresponding encryption process $W = E (Z, K)$ for the processing result Z stored on said memory, and storing the result W on the memory; (3) outputting said processing result Z <u>from said information processing device</u> when said processing result W coincides with said ciphertext C; and (4) <u>suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said ciphertext C</u>.

The invention, as now recited in claim 9, is also directed to a tamper-resistant fault detection method (e.g., Fig. 10; p. 28) for an IC card including an information processing device mounted thereon, comprising the steps of: (1) performing an asymmetric-key decryption process $Z = D (C, X)$ wherein a secret key X is to be applied to an input ciphertext C and storing the result Z in a memory in the IC card; (2) performing a corresponding encryption process $W = E (Z, J)$, wherein a public key J is to be applied to the result Z on said memory and storing said result W on the memory; (3) outputting the processing result Z when said processing result W

coincides with said ciphertext C; and (4) <u>suppressing the output of the processing result Z when said processing result W does not coincide with the ciphertext C</u>.

Applicants respectfully contend that none of the cited prior art references teaches or suggests such a tamper-resistant fault detection method for an IC card including steps of "performing a symmetric-key encryption process in which a secret key K is to be applied to an input plaintext M, and storing a processing result Z <u>in a memory in the IC card</u>; (2) performing a corresponding decryption process $W = D (Z, K)$ for said process result Z stored on said memory 204 and storing the decryption result W on the memory 204; (3) outputting said processing result Z <u>from said information processing device mounted on the IC card</u> when said processing result W coincides with said plaintext M; and (4) <u>suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said plaintext M</u> " as the invention.

In contrast, Blanchard simply does not mention or concern any IC cards, much less about a tamper-resistant fault detection method for an IC card. Blanchard merely produces a data packet consisting of a plaintext M and an error detection data added thereto (step 410 in Fig. 4). Then, Blanchard encrypts the data packet (step 420), and decrypts the encrypted data packet (step 430). The decrypted data packet is expected to contain both the plaintext M and the error detection data. Blanchard judges whether there is an <u>error in the data packet</u> by using the <u>error detection data</u> (steps 450-460; col. 4, line 63 to col. 5, line 1). Such an error is *accidentally* made "during the encryption or decryption (col. 4, lines 66)" and is intended to be prevented from "*inadvertently* transmitted, such as "unencrypted data" (col. 1, lines 15-20). Blanchard's errors are essentially different form the *internationally* generated erroneous operations generated by an IC card attacker. Blanchard does not "(1) perform a symmetric-key encryption process in which a secret key K is to be applied to an input plaintext M, and storing a processing result Z <u>in a memory in the IC card</u>; (2) perform a corresponding decryption process $W = D (Z, K)$ for said process result Z stored on said memory 204 and storing the decryption result W <u>on the memory 204</u>; (3) output said processing result Z <u>from said information processing device mounted on the IC card</u> when said processing result W coincides with said plaintext M; or (4) suppress the output of said processing result Z <u>from said information processing device</u> when said processing result W does not coincide with said plaintext M "

Other cited references fail to compensate for Blanchard's deficiencies in terms of the independent claims as well as the dependant claims as discussed as follows. In particular, Boneh (p. 38, 4th par.) only uses a hardware faulty *attacking* mechanism against RSA implementation in an IC card (Abstract), rather than any *tamper-resistant* (*defending/protecting*) fault detection method for an IC card. It is well established that a rejection based on cited references having principles that teach away from the invention is improper. Applicants further contend that one skilled in the art would not be motivated to combined Boneh and Blanchard as suggested by the Examiner, since their intended purposes (lunching attacks vs. defending attacks) conflict with each other. It is also well established that a rejection based on cited references having contradictory principles is improper.

Even if, arguendo, a person of ordinary skill were motivated to combine the teachings with Blanchard, such combined teachings would still fall short in fully meeting the Applicants' claimed invention as set forth in the independent claims. Boneh merely checks cryptographic protocol for faults, it does not disclose any specific verifying means or mechanism for comparing the result W with the plaintext M stored in a memory in the IC card as the present invention.

Claim 2 recites an instance where the present claim 1 is applied to DES. Fernandez-Gomez merely acquires a cipher text by encrypting a plain text, and then compares a result after decrypting the cipher text with the original plain text (Fig. 7). Fernandez-Gomez, however, does not output the cipher text itself as the processing result, because it intends to detect hardware failures of the cipher mechanism (p. 979, right col., line 11; p. 980, left col., line 4-). As Fernandez-Gomez only intends to gather an error detection probability to see if how many errors are detected on the cipher mechanism, it does not output the cipher text gained as a processing result to the external world. Hence, Fernandez-Gomez fails to teach the present invention in how to control the output of the processing result Z and how to output it when it is correct.

Daniels (Fig. 3) decrypts an encrypted packet by utilizing a master decryption key, encrypts the decrypted packet utilizing an encryption key, and compares the encrypted result with the original encrypted packet. Daniels performs the processing to check security of data received by a computer from a client. Daniels only intends to prevent the data-security-checking software from being damaged by an incoming erroneous packet (col. 1, lines 52-59). Daniels does not disclose the present invention, which controls the output of the processing result Z and

outputs it when it is correct. As such, the combination of Daniels and Fernandez-Gomez does not make the invention obvious.

Claim 3 recites an information processing device being reset when it detects an occurrence of mismatch between the result W and the plaintext M. Ogg only discloses a cryptographic module being reset when it detect any attempts to tamper with the module.

Claim 4 recites the encryption mechanism implemented by an IC card. As mentioned, Boneh only discloses a signature technique using RSA algorithm, not related to DES. Further, Boneh (p38, 4th par.) does not disclose any specific verifying means or mechanism for comparing the result W with the plaintext M as the present invention.

Claims 5-8 outputs a decrypted result Z. As mentioned above, Daniels does not disclose the steps of "controlling the output of the processing result Z and outputting it when it is correct". That is also applicable to the decryption process. As such the combination of Daniels and Fernandez-Gomez does not make the invention obvious.

Claims 9-12 decrypts a ciphertext C by the use of a secret key X to obtain a result Z, and encrypts the result Z by use of public key J to obtain a result W. Daniels does not disclose the steps of "controlling the output of the processing result Z and outputting it when it is correct," and Schneier merely discloses the RSA algorithm. The combination of Daniels and Schneier does not make the invention obvious.

Neither Blanchard, nor its combinations with other cited references teaches or suggests each and every feature of the present invention as recited in independent claims 1, 5, and 9. As such, the present invention as now claimed is distinguishable and thereby allowable over the rejections raised in the Office Action. The withdrawal of the outstanding prior art rejections is in order, and is respectfully solicited.
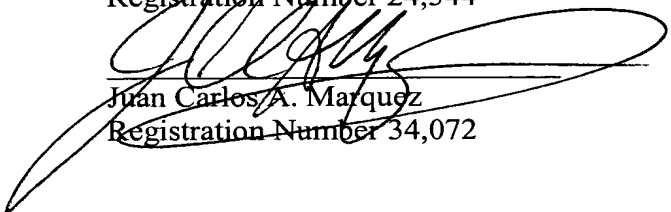

Conclusion

In view of all the above, Applicants respectfully submit that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art references upon which the rejections in the Office Action rely. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor

rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive, Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

February 17, 2005

SPF/JCM/JT